1969

The lattice of intermediate fields of a purely inseparable extension

George Franklin Haddix
Iowa State University

THE LATTICE OF INTERMEDIATE FIELDS OF A PURELY INSEPARABLE EXTENSION

by

George Franklin Haddix

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of
The Requirements for the Degree of
DOCTOR OF PHILOSOPHY

Major Subject: Mathematics

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

Head of Major Department

Signature was redacted for privacy.

Dean of Graduate College

Iowa State University
Of Science and Technology
Ames, Iowa

1969

TABLE OF CONTENTS

I. INTRODUCTION

It is well-known that the intermediate fields of a field extension L of a field K, that is, the fields F such that $K \subseteq F \subseteq L$, form a complete lattice with meet defined as the ordinary set intersection and join defined as the field composite structure. The composite of two intermediate fields F and F' is defined to be the smallest intermediate field containing both F and F'. If L is an algebraic extension of K, which we will denote by L/K, the set S of all elements which are separable over K is an intermediate field of L/K. This subfield S is the maximal separable subfield of L/K, and the only elements of L which are separable over S are elements of S. The extension L/S is called purely inseparable. Thus any algebraic extension L/K can be considered in two stages, a separable stage S/K, and a purely inseparable stage L/S. In this thesis we will be concerned with the lattice of intermediate fields of a purely inseparable extension of characteristic $p \neq 0$.

In [7] Pickert discovers some connections between the lattice of intermediate fields and the structure of the extension. For instance he shows that the lattice of intermediate fields is modular if and only if the extension has multiplicity not greater than two. Multiplicity is defined to be the minimal number of elements one must adjoin

to K in order to generate L. In this thesis we will be concerned with the problem of determining to what extent the lattice of intermediate fields determines the structure of the extension. We approach the problem in the following way: If L/K and L'/K are two purely inseparable extension of characteristic $p \neq 0$ and $\mathfrak{L}$ and $\mathfrak{L}'$ are their respective intermediate field lattices, we suppose that $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic and try to discover properties that the extensions have in common.

In the theory of purely inseparable extensions many results concern generations of the extensions. In particular we notice subbases [10] and minimal generating sets [8]. In [6] and [5] certain canonical generations are shown to exist, and it is shown that certain numerical invariants are associated with the generation. In [9] Sweedler suggests another type of natural generation, which we will pursue further. The main results of this thesis can be roughly described as follows: The lattice of intermediate fields of an extension determines the existence of each of the aforementioned types of generations, and also any numerical invariants associated with the generation.

Chapter II contains the necessary definitions and lemmas, along with the more obvious results concerning minimal generating sets, subbases, and lattice isomorphisms.

In Chapter III it is shown that the lattice of

intermediate fields determines not only the existence of a canonical generating set but also the canonical generating invariants as described in [6] and [5]. The converse of this statement is shown to not be true by example.

In Chapter IV we describe another type of natural generation, and point out a few interesting properties of the generating sets.

In Chapter V we prove that certain numerical invariants analogous to those described in [6] and [5] are associated with the generating sets described in Chapter IV.

In Chapter VI we show that the lattice of intermediate fields determines the numerical invariants derived in Chapter V.

II. PRELIMINARIES

In this chapter we prove the lemmas which lead directly to the proofs of the main theorems of the thesis. We will use the symbol L/K to denote a field extension of the field K. For two extensions L/K and L'/K the lattices of intermediate fields will be denoted by the symbols $\mathfrak{L}$ and $\mathfrak{L}'$ respectively. The symbol $[L:K]$ will denote the vector space dimension of L/K. $|A|$ will denote the cardinality of the set A. We begin by listing definitions and elementary facts which appear in many places in the available literature on field extensions.

Suppose L/K is a purely inseparable field extension of characteristic $p \neq 0$. If $[L:K] < \infty$ we say L/K is a finite dimensional extension. If there exists a nonnegative integer j such that $L^{p^j} \subseteq K$, where $L^{p^j} = \{a^{p^j} : a \in L\}$, we say L/K is of bounded exponent. If L/K is of bounded exponent there exists a minimal integer e such that $L^{p^e} \subseteq K$; this integer is called the exponent of L/K, denoted by $\exp L/K$. When we write $L^{p^e} \subseteq K$ we will always mean that $e = \exp L/K$. It is obvious that $[L:K] < \infty$ implies L/K is of bounded exponent. If $a \in L$, the smallest integer e such that $a^{p^e} \in K$ is called the exponent of a over K, denoted by $\exp a/K$.

Definition 2.1. Let F be a field extension of a field K of characteristic $p \neq 0$. A relative p-basis of F/K is a set $B \subseteq F$ such that $F = F^p(K,B)$ and $b \in B$ implies $b \notin F^p(K, B - b)$.

Here $B - b$ denotes the set difference $B - \{b\}$. The Axiom of Choice insures the existence of a relative p-basis for any extension (not necessarily purely inseparable). Furthermore the cardinality of a relative p-basis is unique.

Definition 2.2. Let F be a field extension of a field K of characteristic $p \neq 0$. A minimal generating set, denoted by m.g.s., of F/K is a subset $M \subseteq F$ such that $F = K(M)$ and $m \in M$ implies $m \notin K(M - m)$.

Remark 2.3. A slight generalization of Proposition 6 [7] shows that if L/K is purely inseparable and $L = K(M)$, then M is a minimal generating set for L/K if and only if M is a relative p-basis for L/K. Hence if $L^{p^e} \subseteq K$ the existence of a minimal generating set of L/K is assured by the existence of a relative p-basis. If L/K is not of bounded exponent the existence of a minimal generating set cannot be assumed.

From here onward L/K will denote a proper purely inseparable extension of characteristic $p \neq 0$.

Definition 2.4. Let L/K be a purely inseparable extension of characteristic $p \neq 0$. A subbasis of L/K is a subset $B \subseteq L - K$ such that $L = K(M)$ and for any subset $\{b_1,\ldots,b_n\}$ the natural homomorphism of $K(b_1) \otimes_K K(b_2) \otimes_K \ldots \otimes_K K(b_n)$ onto $K(b_1,\ldots,b_n)$ is one-one.

Here the symbol $A \otimes_K B$ denotes the tensor product over K. Some conditions for the existence of a subbasis appear for instance in [1], [9], and [10]. The name "modular extension" has been used to denote an extension which has a subbasis.

The following lemma is a combination of Satz 6 [5] and Theorem 15 page 55 [2]. However, a proof is given here for the convenience of the reader.

Lemma 2.5. Let L/K be a purely inseparable extension such that $[L:K] = p^e$, $e > 0$. Then L/K is a simple extension if and only if there exist only a finite number of intermediate fields of L/K. Furthermore if $L = K(b)$ the fields $K(b^{p^i})$, $i = 1,\ldots,e - 1$ are the intermediate fields of L/K.

Proof: First suppose $L = K(b)$ and let G be an intermediate field of L/K. Then $[G:K] = p^j$ for some $1 \leq j \leq e - 1$, and hence $[L:G] = p^{e-j}$. Thus $b^{p^{e-j}} \in G$

and $K(b^{p^{e-j}}) \subseteq G$. Therefore, since $b^{p^e} \in K - K^p$ we have the degree relation $[K(b^{p^{e-j}}) : K] = p^j = [G:K]$. Thus any linear basis of $K(b^{p^{e-j}})/K$ is a linear basis of $G|K$ and we must have $K(b^{p^{e-j}}) = G$. Note that this also proves the last sentence in the statement of the lemma. Next suppose there exists only a finite number of fields between K and L. We will see that if $a, b \in L$ then $K(a,b)$ is a simple extension. Consider the set of intermediate fields $\{K(a + bc) : c \in K\}$. K is infinite since it admits a purely inseparable extension. Hence there exist $c, d \in K$ such that $c \neq d$ and $K(a + cb) = K(a + db)$. Then we have $b = (c - d)^{-1}[(a + cb) - (a + db)] \in K(a + cb)$, and hence $a = (a + cb) - cb \in K(a + cb)$. Thus $K(a,b) = K(a + cb)$.

Q.E.D.

We note that the above lemma points out in particular that L/K is a simple extension if and only if $\mathfrak{L}$ is a finite chain.

Lemma 2.6. Let L/K and L'/K be two purely inseparable extensions of K. If $L = K(b)$ for some $b \in L$, $[L:K] = p^e$, $e > 0$, and f is an isomorphism between $\mathfrak{L}$ and $\mathfrak{L}'$, then

(1) There exists $b' \in L'$ such that $L' = K(b')$,

(2) $[L':K] = p^e$, and

(3) $f(K(b^{p^i})) = K(b'^{p^i})$.

Proof: (1) By Lemma 2.5 the only fields between K and L are the fields $K(b^{p^i})$, $i = 1,\ldots,e-1$. Hence there must exist $e-1$ fields between K and L' or we contradict the one-oneness of f. Then again by Lemma 2.5 there exists a $b' \in L'$ such that $L = K(b')$.

(2) By Lemma 2.5 and (1) the only intermediate fields of L'/K are $K(b'^{p^i})$, $i = 1,\ldots,e'-1$, where $e' = \exp b'|K$. The one-oneness of f obviously implies $e = e'$.

(3) Since we have the chains
$K \subset K(b^{p^{e-1}}) \subset \ldots \subset K(b^p) \subset L$ and
$K \subset K(b'^{p^{e-1}}) \subset \ldots \subset K(b'^p) \subset L$ it is clear that
$f(K(b^{p^i})) = K(b'^{p^i})$, $i = 0,\ldots,e$. Q.E.D.

We are now ready to prove a theorem that is indicative of the type of results we hope to prove throughout the thesis. We again remind the reader that the existence of a minimal generating set for L/K cannot be assumed when L/K is of unbounded exponent.

Theorem 2.7. Let f be an isomorphism between $\mathfrak{L}$ and $\mathfrak{L}'$. If L/K has a minimal generating set M, then L'/K has a minimal generating set M' such that $m' \in M'$ implies there exists $m \in M$ such that $f(K(m)) = K(m')$,

and $|M| = |M'|$.

Proof: By Lemma 2.6, for each $m \in M$ we can and do choose a $m' \in L'$ such that $f(K(m)) = K(m')$. Denote the set of m''s so chosen by M'. Now define a map $g : M \to M'$ as follows: $g(m) = m'$ if and only if $f(K(m)) = K(m')$. It is clear that g is onto M'. Now suppose m_1 and m_2 are elements of M such that $m_1 \neq m_2$. Since M is a m.g.s. $K(m_1) \neq K(m_2)$. The one-oneness of f implies $f(K(m_1)) \neq f(K(m_2))$, and hence $g(m_1) \neq g(m_2)$. Thus g is one-one and $|M| = |M'|$. Since f preserves l.u.b.'s we must have

$$L' = f(L) = f(\text{l.u.b.}\{K(m) : m \in M\})$$

$$= \text{l.u.b.}\{f(K(m)) : m \in M\}$$

$$= \text{l.u.b.}\{K(m') : m' \in M'\} = K(M').$$

Hence M' generates L'/K. Now suppose M' is not a m.g.s., that is, there exists $m'_o \in M'$ such that $L' = K(M' - m'_o)$. If $m_o \in M$ is such that $f(K(m_o)) = K(m'_o)$, then we must have $f(K(M - m_o)) = f(\text{l.u.b.}\{K(m) : m \in M - m_o\}) = \text{l.u.b.}\{f(K(m)) : m \in M - m_o\} = \text{l.u.b.}\{K(m') : m' \in M' - m'_o\} = K(M' - m'_o) = L'$. However, this contradicts the one-oneness of f since $K(M - m_o) \neq L$.

Q.E.D.

We get a similar result concerning subbases in the following theorem.

Theorem 2.8. Let f be an isomorphism between $\mathfrak{L}$ and $\mathfrak{L}'$. If L/K has a subbasis B, then L'/K has a subbasis B', and $|B| = |B'|$.

Proof: By an argument totally similar to that of Theorem 2.7 we pick a set $B' \subseteq L'$ such that $K(B') = L'$ and such that there exists a one-one function $g : B \to B'$ defined by $g(b) = b'$ if and only if $f(K(b)) = K(b')$. By the one-oneness of f and Lemma 2.5 we must have that if $g(b) = b'$ then $\exp b/K = \exp b'/K$. Let $b'_o \in B'$, $b_o \in B$ such that $g(b_o) = b'_o$, and $e = \exp b_o/K = \exp b'_o/K$. Since f preserves l.u.b.'s we must have $f(K(B - b_o)) = K(B' - b'_o)$. Let $\exp b'_o/K(B' - b'_o) = e'$. Then $[L':K(B' - b'_o)] = p^{e'}$. By Lemma 2.5 $K(B' - b'_o)(b'_o{}^{p^i})$, $i = 1,\ldots,e' - 1$ are the only fields between $K(B' - b'_o)$ and L', and $K(b_o^{p^i})$, $i = 1,\ldots,e - 1$ are the only fields between $K(B - b_o)$ and L. Hence since f is one-one we must have $e = e'$. Q.E.D.

Lemma 2.9. Let f be an isomorphism of $\mathfrak{L}$ to $\mathfrak{L}'$. If F and G are intermediate fields such that $F \subseteq G$ and $\exp G/F = e$ then $\exp f(G)/f(F) = e$. Furthermore, $f(F(G^{p^i})) = F'(G'^{p^i})$, $i = 0,1,\ldots,$ where $F' = f(F)$ and

$G' = f(G)$.

Proof: Let $a \in G - F$ such that $\exp a/F = e$. Then we have the degree relation $[F(a) : F] = p^e$. By Lemma 2.5 the only fields between F and $F(a)$ are the fields $F(a^{p^i})$, $i = 1,\ldots,e - 1$. Hence there exist only $e - 1$ fields between F' and $f(F(a))$. Lemma 2.6 implies there exists an $a' \in G'$ such that $f(F(a)) = F'(a')$ and $\exp a'/F' = e$. Hence $\exp G'/F' \geq e$. However, since f^{-1} is an isomorphism of $\mathfrak{L}'$ to $\mathfrak{L}$, a similar use of Lemmas 2.5 and 2.6 implies that $\exp G'/F' \leq e$.

Now suppose $H \in \mathcal{H} = \{H : F \subseteq H \subseteq G, \exp G/H \leq i\}$. Then $g \in G$ implies $g^{p^i} \in H$ and hence $F(G^{p^i}) \subseteq H$. Clearly $F(G^{p^i}) \in \mathcal{H}$. This proves that $F(G^{p^i}) = \text{g.l.b.}\mathcal{H}$. From the previous paragraph it is obvious that

$$\{H' : F' \subseteq H' \subseteq G', \exp G'/H' \leq i\} =$$

$$\{f(H) : F \subseteq H \subseteq G, \exp G/H \leq i\}.$$

Hence since f preserves g.l.b.'s,

$$F'(G'^{p^i}) = \text{g.l.b.}\{H' : F' \subseteq H' \subseteq G',\ \exp G'/H' \leq i\}$$

$$= \text{g.l.b.}\{f(H) : F \subseteq H \subseteq G,\ \exp G/H \leq i\}$$

$$= f(\text{g.l.b.}\{H : F \subseteq H \subseteq G,\ \exp G/H \leq i\}$$

$$= f(F(G^{p^i})).$$

Q.E.D.

Before proceeding to the next theorem we take time to introduce some convenient notation. For a given extension L/K the chain of fields

$$L \supseteq K(L^p) \supseteq \ldots \supseteq K(L^{p^j}) \supseteq K(L^{p^{j+1}}) \supseteq \ldots \supseteq K$$

will be called the <u>left basic chain of L/K</u>, denoted by L.B.C.. Of course if $L^{p^e} \subseteq K$ then $j < e$ and the chain is finite. We let

$$L_i = K^{p^{-i}} \cap L = \{\ell \in L : \ell^{p^i} \in K\}, \quad i = 0, 1, \ldots .$$

It is clear that $L_i \subseteq L_{i+j}$ for $j \geq 0$, and that $L_{i+j}^{p^j} \subseteq L_i$ for $j \geq 0$. The chain of fields

$$K = L_o \subseteq L_1 \subseteq \cdots \subseteq L_j \subseteq L_{j+1} \subseteq \cdots \subseteq L$$

will be called the <u>right basic chain of L/K</u>, denoted by R.B.C.. Again if $L^{p^e} \subseteq K$ the chain is finite with $e + 1$ elements. Finally let $L_{i,j} = L_{i-1}(L_j^{p^{j-i}})$ for $j > i$, $i \geq 1$. Then for each i the chain of fields

$$L_i \supseteq L_{i,i+1} \supseteq \cdots \supseteq L_{i,j-1} \supseteq L_{i,j} \supseteq \cdots \supseteq L_{i-1}$$

will be called the <u>ith basic subchain of L/K</u>. The chain of fields

$$K = L_o \subseteq \cdots \subseteq L_{1,j} \subseteq L_{1,j-1} \subseteq \cdots \subseteq L_{1,3} \subseteq L_{1,2} \subseteq$$
$$L_1 \subseteq \cdots \subseteq L_{2,j} \subseteq L_{2,j-1} \subseteq \cdots \subseteq L_{2,4} \subseteq L_{2,3} \subseteq L_2 \subseteq \cdots \subseteq L_i$$
$$\subseteq \cdots \subseteq L_{i+1,j} \subseteq L_{i+1,j-1} \subseteq \cdots \subseteq L_{i+1,i+3} \subseteq L_{i+1,i+2} \subseteq L_{i+1}$$
$$\subseteq \cdots \subseteq L_{j-3} \subseteq \cdots \subseteq L_{j-2,j} \subseteq L_{j-2,j-1} \subseteq L_{j-2} \subseteq \cdots \subseteq L_o = L.$$

will be called the <u>refined right basic chain of L/K</u>. If $L^{p^e} \subseteq K$ then the union of the R.B.C. and L.B.C. form a sublattice of $\mathfrak{L}$. This lattice will be called the <u>basic sublattice of $\mathfrak{L}$</u> and is illustrated in the following diagram.

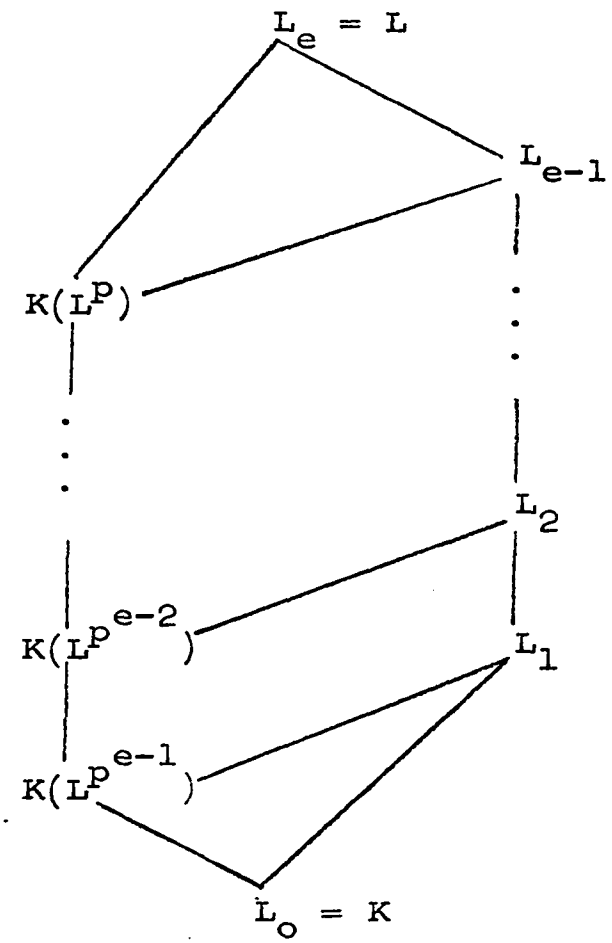


Diagram 2.10

Theorem 2.11. Let f be an isomorphism of $\mathfrak{L}$ to $\mathfrak{L}'$. Then $f(K(L^{p^i})) = K(L'^{p^i})$, $f(L_i) = L'_i$, and $f(L_{i,j}) = L'_{i,j}$, $i = 0,1,\ldots,$ $j > i$.

Proof: Suppose $F \in \mathfrak{F} = \{F : K \subseteq F \subseteq L,\ \exp F/K \leq i\}$. Then $a \in F$ implies $a^{p^i} \in K$ and hence $F \subseteq L_i$. Clearly $L_i \in \mathfrak{F}$. By Lemma 2.9

$$\{F' : K \subseteq F' \subseteq L',\ \exp F'/K \leq i\} =$$

$$\{f(F) : K \subseteq F \subseteq L,\ \exp F/K \leq i\}.$$

Hence since f preserves l.u.b.'s $f(L_i) = L'_i$. Now $f(K(L^{p^i})) = K(L'^{p^i})$ and $f(L_{i,j}) = L'_{i,j}$ are immediate from Lemma 2.9. Q.E.D.

Corollary 2.12. Let f be an isomorphism of $\mathfrak{L}$ to $\mathfrak{L}'$. Then f induces an isomorphism between the following sublattices of $\mathfrak{L}$ and $\mathfrak{L}'$.

(1) the R.B.C. of L/K and the R.B.C. of L'/K,

(2) the L.B.C. of L/K and the L.B.C. of L'/K,

(3) the ith basic subchain of L/K and the ith basic subchain of L'/K, and

(4) the refined basic chains of L/K and L'/K.

Furthermore, if $L^{p^e} \subseteq K$ f induces an isomorphism between the basic sublattices of $\mathfrak{L}$ and $\mathfrak{L}'$.

Proof: Immediate from the theorem and definitions.

III. CANONICAL GENERATING SETS AND LATTICE ISOMORPHISMS

In [6] Pickert shows that certain numerical invariants are associated with a canonical generation of L/K when $[L:K] < \infty$. In [2] and [5] the result is extended to the bounded and unbounded exponent cases respectively. In this chapter we will show that if $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic then L/K and L'/K have the same canonical generating invariants. The following is Corollary A in [5].

Theorem 3.1. If there exist subsets M_i in L such that $M_i^{p^i}$ is a minimal generating set of $K(L^{p^i})/K$, $i = 0,1,\ldots$, then there exist disjoint subsets $B_i \subseteq L$ and positive integers e_i, $i = 1,2,\ldots$ such that:

(a) $\bigcup_{i=1}^{\infty} B_i = M_o$ and for $i = 1,2,\ldots$

(1) $B_i^{q_i} \subseteq K(B_{i+1}^{q_i}, B_{i+2}^{q_i}, \ldots)$ where $q_i = p^{e_i}$

(2) For all $B_i' \subseteq B_i$ and $b \in B_i - B_i'$, b has exponent e_i over $K(B_i', B_{i+1}, \ldots)$

(3) $e_1 < e_2 < \ldots$

(b) $\bigcup_{j=1}^{\infty} B_j^{q_i}$ is p-independent in $K(L^{q_i})$, $i = 1,2,\ldots$

(c) The e_i's and the cardinalities of B_i, $\{B_i\}$ and M_{i-1}, $i = 1,2,\ldots$ are invariants of the extension.

Definition 3.2. If $B_1, B_2, \ldots$ are subsets of L which satisfy the conditions of (a) of 3.1, then $\{B_1, B_2, \ldots\}$ is called the canonical generating system for L/K. The elements of $\bigcup_{i=1}^{\infty} B_i$ are called canonical generators, and L is said to be canonically generated.

We will use the symbol c.g.s. to denote a canonical generating system. If two extensions L/K and L'/K have c.g.s.'s $\{B_1, B_2, \ldots\}$ and $\{B_1', B_2', \ldots\}$ respectively, we say that L/K and L'/K have the same canonical generating invariants if and only if for all $i = 1,2,\ldots$ $|B_i| = |B_i'|$ and $e_i = e_i'$, where e_i and e_i' are the exponents corresponding to B_i and B_i' respectively.

Theorem 3.3. Suppose $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic. If L/K has a canonical generating system, then L'/K has a canonical generating system and L/K and L'/K have the same canonical generating invariants.

Proof: Let $f : \mathfrak{L} \to \mathfrak{L}'$ be an isomorphism and $\{B_1, B_2, \ldots\}$ be a c.g.s. for L/K. $M = B_1 \cup B_2 \cup \ldots$ is a m.g.s. for L/K and hence by Theorem 2.7 there exists a m.g.s. M' for L'/K such that $m' \in M'$ implies there exists a unique $m \in M$ such that $f(K(m)) = K(m')$. Partition M' into $M' = B_1' \cup B_2' \cup \ldots$ as follows:

$B_i' = \{b' \in M' :$ there exists a $b \in B_i$ such that $f(K(b)) = K(b')\}$. It is clear from the construction that $|B_i| = |B_i'|$, $i = 1,2,\ldots$. For all $i = 1,2,\ldots$, let $K_i = K(B_{i+1}, B_{i+2}, \ldots)$ and $K_i' = K(B_{i+1}', B_{i+2}', \ldots)$. Then $K_i = \text{l.u.b.}\{K(b) : b \in B_{i+1} \cup B_{i+2} \cup \ldots\}$ and $K_i' = \text{l.u.b.}\{K(b') : b' \in B_{i+1}' \cup B_{i+2}' \cup \ldots\}$. Since $b' \in B_{i+1}' \cup B_{i+2}' \cup \ldots$ if and only if there exists $b \in B_{i+1} \cup B_{i+2} \cup \ldots$ such that $f(K(b)) = K(b')$ and since f preserves l.u.b.'s we have $f(K_i) = K_i'$. Similarly if $D_i \subseteq B_i$ we have $f(K(D_i)) = K(D_i')$ where $D_i' \subseteq B_i'$ such that $b' \in D_i'$ if and only if there exists $b \in D_i$ such that $f(K(b)) = K(b')$. Thus if $b' \in B_i' - D_i'$ we must have by Lemma 2.6 and the one-oneness of f that

$$[K(D_i \cup B_{i+1} \cup B_{i+2} \cup \ldots, b) : K(D_i \cup B_{i+1} \cup B_{i+2} \cup \ldots)] =$$

$$[K(D_i' \cup B_{i+1}' \cup B_{i+2}' \cup \ldots, b') : K(D_i' \cup B_{i+1}' \cup B_{i+2}' \cup \ldots)]$$

where $f(K(b)) = K(b')$. Another application of Lemma 2.6 shows that

$$e_i = \exp b/K(D_i \cup B_{i+1} \cup B_{i+2}, \ldots) =$$

$$\exp b'/K(D_i' \cup B_{i+1}' \cup B_{i+2}' \cup \ldots).$$

This shows that the B_i', $i = 1,2,\ldots$ satisfy (2) and (3) of Theorem 3.1 (a).

By Lemma 2.9

$$f(K(B_{i+1}^{q_i}, B_{i+2}^{q_i}, \ldots)) = K(B_{i+1}'^{q_i}, B_{i+2}'^{q_i}, \ldots) \quad \text{and}$$

$$f(K(B_{i+1}^{q_i}, B_{i+2}^{q_i}, \ldots, b_i)) = K(B_{i+1}'^{q_i}, B_{i+2}'^{q_i}, \ldots, b_i')$$

where $q_i = p^{e_i}$, e_i is the canonical exponent corresponding to B_i, and $f(K(b_i)) = K(b_i')$. It follows immediately from the one-oneness of f and Lemma 2.5 that

$$\exp b'/K(B_{i+1}'^{q_i}, B_{i+2}'^{q_i}, \ldots) = e_i = \exp b/K(B_{i+1}^{q_i}, B_{i+2}^{q_i}, \ldots).$$

Hence $\{B_1', B_2', \ldots\}$ is a c.g.s. of L'/K and L/K and L'/K have the same canonical generating invariants. Q.E.D.

We now show that the converse of Theorem 3.3 is not true.

Example 3.4. When L/K and L'/K have the same canonical generating invariants, $\mathfrak{L}$ and $\mathfrak{L}'$ need not be isomorphic. Let P be a perfect field of prime characteristic and x, y, and z be algebraically independent indeterminants over P. Set

$K = P(x,y,z)$, $L = K(x^{p^{-2}}, y^{p^{-1}})$, and $L' = K(x^{p^{-2}}, x^{p^{-2}}y^{p^{-1}} + z^{p^{-1}})$. Now if one sets $\{y^{p^{-1}}\} = B_1$ and $\{x^{p^{-2}}\} = B_2$ we have $B_1^p \subset K(B_2^p)$. Since x and y are independent $y^{p^{-1}} \notin K(B_2)$, so $\exp y^{p^{-1}}/K(B_2) = 1$ while $\exp x^{p^{-2}}/K = 2$. Hence $\{B_1, B_2\}$ is a c.g.s. of L/K with $|B_1| = 1$, $|B_2| = 1$, $e_1 = 1$, and $e_2 = 2$. If we set $\{x^{p^{-2}}\} = B_1'$ and $\{x^{p^{-2}}y^{p^{-1}} + z^{p^{-1}}\} = B_2'$ we have $B_1'^p \subseteq K(B_2'^p)$. However, $x^{p^{-2}} \notin K(B_2')$, so $\exp x^{p^{-2}}/K(B_2') = 1$ while $\exp x^{p^{-2}}y^{p^{-1}} + z^{p^{-1}}/K = 2$. Hence $\{B_1', B'_2\}$ is a c.g.s. for L'/K with $|B_1'| = 1$, $|B_2'| = 1$, $e_1' = 1$, and $e_2' = 2$. We have actually seen above that $\{x^{p^{-2}}, y^{p^{-1}}\}$ is a subbasis of L/K. However, L'/K does not have a subbasis by, for instance, Exercise 6 of [3, p.196] or Example 1.1 of [9, p.405]. Thus by Theorem 2.8 the lattices of intermediate fields are not isomorphic.

IV. TOWER SETS AND TOWER GENERATING SETS

In [9] Sweedler gives a construction of a generating set when $L^{p^e} \subseteq K$. The construction is as follows. Consider the R.B.C. of L/K, $K = L_o \subseteq L_1 \subseteq \ldots \subseteq L_{e-1} \subseteq L_e = L$. Let $S_{e,e}$ be a p-basis of L_e/L_{e-1}. Then let $S_{e-1,e} \subseteq S^p_{e,e}$ be a maximal p-independent subset of $S^p_{e,e}$ over L_{e-2}, and let $S_{e-1,e-1}$ be an augmentation of $S_{e-1,e}$ to a p-basis of L_{e-1}/L_{e-2}. Now suppose that we have constructed the set

$$S_{e-i,e-i} \cup S_{e-i,e-i+1} \cup \ldots \cup S_{e-i,e-1} \cup S_{e-i,e}$$

a p-basis of L_{e-i}/L_{e-i-1}. Let T be a maximal p-independent set over L_{e-i-2} contained in

$$S^p_{e-i,e-i} \cup S^p_{e-i,e-i+1} \cup \ldots \cup S^p_{e-i,e-1} \cup S^p_{e-i,e}.$$

Let

$$S_{e-i-1,j} = S^p_{e-i,j} \cap T$$

for $j = e,\ldots,e-i$, and let $S_{e-i-1,e-i-1}$ be an augmentation of T to a p-basis of L_{e-i-1}/L_{e-i-2}. The procedure terminates with the construction of the set

$$S_{1,1} \cup S_{1,2} \cup \ldots \cup S_{1,e}$$

a p-basis of L_1/L_o. It is clear from the construction that $S_{i,i} \cap S_{j,j} = \emptyset$ if $i \neq j$. It is easily seen in Lemma 0 [9, p.402], that $\{\pi x^{j(x)} : x \in \bigcup_{i=1}^{e} S_{i,i}$, $0 \leq j(x) < p^{k+1}$, where k is a maximal integer such that $x^{p^k} \in S_{i-k,i}$ when $x \in S_{i,i}\}$ is a linear basis of for L/K. Thus the set $N = \bigcup_{j=1}^{e} S_{j,j}$ is a generating set for L/K. We now pause to note a few facts about the generating set $N = \bigcup_{i=1}^{e} S_{i,i}$.

Proposition 4.1. If

$$N = \bigcup_{i=1}^{e} S_{i,i}$$

and

$$N' = \bigcup_{i=1}^{e} S'_{i,i}$$

are two generating sets constructed as above then

$$|S_{i,i}| = |S'_{i,i}|$$

for all $i = 1,\ldots,e$.

Proof: Since

$$S_{i,i+1} \cup S_{i,i+2} \cup \ldots \cup S_{i,e}$$

is a maximal p-independent set of

$$S^p_{i+1,i+1} \cup S^p_{i+1,i+2} \cup \ldots \cup S^p_{i+1,e}$$

we have

$$L_i(S_{i,i+1}, S_{i,i+2}, \ldots, S_{i,e})$$

$$= L_i(S^p_{i+1,i+1}, S^p_{i+1,i+2}, \ldots, S^p_{i+1,e}).$$

However

$$L_i(S^p_{i+1,i+1}, \ldots, S^p_{i+1,e})$$

$$= L_i(L^p_{i+1})(S^p_{i+1,i+1}, \ldots, S^p_{i+1,e})$$

$$= L_i(L^p_{i+2}).$$

The last equality holds since

$$L_{i+2} = L_{i+1}(S_{i+1,i+1},\ldots,S_{i+1,e}).$$

Hence $S_{i,i}$ is a m.g.s. for

$$L_{i+1}/L_i(L_{i+2}^p).$$

Similarly $S'_{i,i}$ is a m.g.s. for

$$L_{i+1}/L_i(L_{i+2}^p).$$

Q.E.D.

We now note that Example 1.3 of [9, p.406] shows that a generating set N constructed as above need not be a m.g.s.. However, we do have the following result.

Proposition 4.2. If $[L:K] < \infty$ and there exists a generating set N constructed as above such that N is a m.g.s., then every generating set so constructed is a m.g.s..

Proof: Suppose

$$N = \bigcup_{i=1}^{e} S_{i,i}$$

and

$$N' = \bigcup_{i=1}^{e} S'_{i,i}$$

are two generating sets. By Proposition 4.2 $|S_{i,i}| = |S'_{i,i}|$. Hence, since the $S_{i,i}$'s are disjoint, $|N| = |N'|$. Suppose $N'_o \subset N'$ is a m.g.s., then $|N'_o| < |N'|$. This contradicts the uniqueness of the cardinality of a m.g.s..

Q.E.D.

We now give a construction which in the bounded exponent case is a special case of the construction given above. However, this construction has certain advantages. Namely, it can be carried out when L/K is not of bounded exponent, and it gives rise to a set of numerical invariants of the extension L/K which are similar to those considered in [6], [2], and [5]. In Chapter VI it is shown that these invariants are necessarily preserved under lattice isomorphisms. Before giving the construction we first prove the following useful proposition.

Proposition 4.3. Suppose K, G, L are fields such that $K \subseteq G \subseteq L$ and $L^p \subseteq K$. Then if B_1 is a subbasis of G/K and B_2 is a subbasis of L/G, $B_1 \cup B_2$ is a subbasis of L/K.

Proof: Consider the set $\mathfrak{B} = \{B : B \subseteq B_1 \cup B_2,\ B_1 \subseteq B,$ and B is a subbasis for $K(B)/K\}$. An application of Zorn's Lemma shows $\mathfrak{B}$ has a maximal element B. Suppose $K(B) \neq L$. Then there exists a $b \in B_2$ such that $b \notin K(B)$. Since $B \cup \{b\}$ is not a subbasis of $K(B,b)/K$ there must exist a $b' \in B_1$ such that $b' \in K(B - b', b)$. Then

$$b' = \sum k_j \pi b_{i,j}^{f_{i,j}}$$

where $k_j \in K$, $b_{i,j} \in \{B - b'\} \cup \{b\}$, and $0 \leq f_{i,j} < p$. Hence

$$\sum k_j \pi b_{i,j}^{f_{i,j}} - b' = 0.$$

However, this contradicts that the set

$\{ \pi_{b \in B_2} b^{f(b)} : 0 \leq f(b) < p,$ and $f(b) = 0$ for all but a finite number of $b \in B_2\}$ is a linear basis of L/G. Hence $L = K(B)$. Since $K(B_1) = G$, $B_2 \subseteq B$ or we contradict B_2 is a subbasis of L/G. Thus $B = B_1 \cup B_2$. Q.E.D.

Proposition 4.3 will be used often. However, since its use is rather obvious, it will not always be referred to specifically. We note here that if $L^p \subseteq K$, then B is a p-basis of L/K if and only if B is a subbasis for L/K if and only if B is a m.g.s. of L/K.

In order to describe the aforementioned construction we consider the refined right basic chain of L/K. Let $T_{1,1}$ be a p-basis of $L_1/L_{1,2}$. For each positive integer j let $T_{j,j}$ be a p-basis of $L_j/L_{j,j+1}$. Then since $L_{j-1}^p \subseteq L_{j-2}$,

$$\begin{aligned} L_{j-1,j+1}(T_{j,j}^p) &= L_{j-2}(L_{j+1}^{p^2})(T_{j,j}^p) \\ &= L_{j-2}(L_{j-1}^p(L_{j+1}^{p^2})(T_{j,j}^p)) \\ &= L_{j-2}(L_j^p) \\ &= L_{j-1,j}. \end{aligned}$$

Hence we can choose a p-basis $T_{j-1,j} \subseteq T_{j,j}^p$ of $L_{j-1,j}/L_{j-1,j+1}$, that is, $T_{j-1,j}$ is a p-basis of

$$L_{j-2}(L_{j+1}^{p^2})(T_{j,j}^p)/L_{j-2}(L_{j+1}^{p^2}).$$

Now suppose n is an integer such that $i \leq n \leq j-2$, and that we have chosen

$$T_{j-n,j} \subseteq T_{j-n+1,j}^p \subseteq \cdots \subseteq T_{j-1,j}^{p^{n-1}} \subseteq T_{j,j}^{p^n}$$

such that $T_{j-n,j}$ is a p-basis of $L_{j-n,j}/L_{j-n,j+1}$. Then

$$L_{j-n-1,j+1}(T^p_{j-n,j}) = L_{j-n-1,j+1}(L^p_{j-n-1})(T^p_{j-n,j})$$

$$= L_{j-n-2}(L^p_{j-n-1}(L^{p^{n+2}}_{j+1})(T^p_{j-n,j}))$$

$$= L_{j-n-2}(L^p_{j-n,j})$$

$$= L_{j-n-2}(L^{p^{n+1}}_{j})$$

$$= L_{j-n-1,j}.$$

Hence we can choose a p-basis $T_{j-n-1,j} \subseteq T^p_{j-n,j}$ of $L_{j-n-1,j}/L_{j-n-1,j+1}$. Thus for each positive integer j (if $L^{p^e} \subseteq K$, then $j < e$) we can construct the sequence of sets

$$T_{1,j}, T_{2,j}, \ldots, T_{j-1,j}, T_{j,j}$$

such that for each integer $1 \leq n \leq j - 1$, $T_{j-n,j} \subseteq T^p_{j-n+1,j}$ and is a p-basis of $L_{j-n,j}/L_{j-n,j+1}$, and $T_{j,j}$ is a p-basis of $L_j/L_{j,j+1}$.

If $L^{p^e} \subseteq K$ we have a special case when $j = e$.

In this case let $T_{e,e}$ be a p-basis of L_e/L_{e-1}. Since

$$L_{e-2}(T_{e,e}^p) = L_{e-2}(L_{e-1}^p(T_{e,e}^p)) = L_{e-1,e},$$

we may choose a p-basis $T_{e-1,e} \subseteq T_{e,e}^p$ of $L_{e-1,e}/L_{e-2}$. Suppose n is an integer $i \leq n \leq e-2$ and that we have chosen

$$T_{e-n,e} \subseteq T_{e-n+1,e}^p \subseteq \cdots \subseteq T_{e,e}^{p^n}$$

such that $T_{e-n,e}$ is a p-basis of $L_{e-n,e}/L_{e-n-1}$. Then

$$L_{e-n-2}(T_{e-n,e}^p) = L_{e-n-1,e},$$

and we can choose a p-basis $T_{e-n-1,e} \subseteq T_{e-n,e}^p$ of $L_{e-n-1,e}/L_{e-n-2}$. Thus we construct the sequence

$$T_{1,e}, T_{2,e}, \ldots, T_{e-1,e}, T_{e,e}$$

such that for each integer n, $1 \leq n \leq e-1$,

$$T_{e-n,e} \subseteq T_{e-n+1,e}^p \subseteq \cdots \subseteq T_{e,e}^{p^n}$$

and is a p-basis of $L_{e-n,e}/L_{e-n-1}$ and such that $T_{e,e}$ is a p-basis of L_e/L_{e-1}.

Now for each j we can think of the construction of the sequence

$$T_{j,j}, T_{j-1,j}, \ldots, T_{1,j}$$

as the filling in of the j-th column in a triangular array of sets. The triangular array is illustrated in Diagram 4.4.

$$\begin{array}{ccccccccc}
 & & & & & & T_{j+1,j+1} & \cdots \\
 & & & & & T_{j,j} & T_{j,j+1} & \cdots \\
 & & & & & T_{j-1,j} & T_{j-1,j+1} & \cdots \\
 & & & & & \vdots & \vdots & \cdots \\
 & & & & & \vdots & \vdots & \cdots \\
 & & & & & \vdots & \vdots & \cdots \\
 & & T_{3,3} & T_{3,4} & \cdots & T_{3,j} & T_{3,j+1} & \cdots \\
 & T_{2,2} & T_{2,3} & T_{2,4} & \cdots & T_{2,j} & T_{2,j+1} & \cdots \\
T_{1,1} & T_{1,2} & T_{1,3} & T_{1,4} & \cdots & T_{1,j} & T_{1,j+1} & \cdots
\end{array}$$

Diagram 4.4.

Definition 4.5. A triangular array constructed as above will be called a tower triangle. The set

$$T = \bigcup_{i=1}^{\infty} T_{i,i}$$

will be called a tower set. If $L = K(T)$, the triangular array will be called a tower generating triangle and T will be called a tower generating set.

Suppose that for a given tower triangle and each integer i, $\bigcup_{j=i}^{\infty} T_{i,j}$ generates L_i/L_{i-1}. (If $L^{p^e} \subseteq K$, $0 < i \leq e$.) Given $a \in L$, let $k = \exp a/K$. Then $a \in L_k$, and there exists an integer r such that $a \in L_{k-1}(\bigcup_{j=k}^{r} T_{k,j})$. Thus $a \in K(\bigcup_{i=1}^{k} \bigcup_{j=1}^{\infty} T_{i,j})$. However, $T_{i,j} \subseteq T_{j,j}^{p^{j-i}}$, so $a \in K(\bigcup_{j=1}^{\infty} T_{j,j})$. (If $L^{p^e} \subseteq K$, $a \in K(\bigcup_{j=1}^{e} T_{j,j})$.) Hence the given tower triangle is a tower generating triangle. It follows immediately from Proposition 4.3 and the construction that if $L^{p^e} \subseteq K$, then every tower triangle is a tower generating triangle. It is obvious that if $L^{p^e} \subseteq K$ the construction of a tower triangle is a special case of the construction given by Sweedler in [9] and discussed earlier in this chapter. In particular we note that

$S_{j,j} = T_{j,j}$ for all $1 \leq j \leq e$ and $T_{i,j} = \emptyset$ for $j \geq i > e$.

V. TOWER INVARIANTS

In this chapter we show that certain numerical invariants are associated with the tower triangles of an extension L/K.

Theorem 5.1. If τ and τ' are two tower triangles of the extension L/K, then

$$|T_{i,j}| = |T'_{i,j}|, \tag{1}$$

and

$$|T^p_{i+1,j} - T_{i,j}| = |T'^p_{i+1,j} - T'_{i,j}|, \tag{2}$$

where $T_{i,j}$ and $T'_{i,j}$ denote the (i,j)-th entries of τ and τ' respectively.

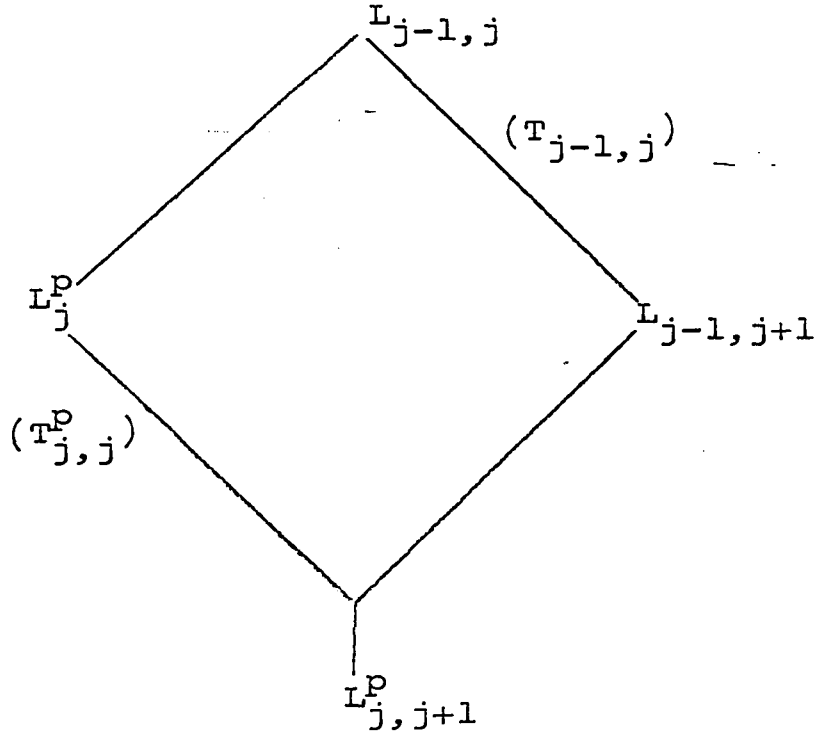
Proof:

$$|T_{i,j}| = |T'_{i,j}|$$

since $T_{i,j}$ and $T'_{i,j}$ are both p-bases of the same extension. Now let j be a positive integer such that $j > 1$. Then $T_{j,j}$ is a p-basis of $L_j/L_{j,j+1}$. Hence $T^p_{j,j}$ is a p-basis of $L^p_j/L^p_{j,j+1}$. $T_{j-1,j}$ is a p-basis for

$$L_{j-1,j}/L_{j-1,j+1}$$

and we have the following lattice diagram:



Similarly $T'^p_{j,j}$ is a p-basis for $L^p_j/L^p_{j,j+1}$, and $T'_{j-1,j}$ is a p-basis of $L_{j+1,j}/L_{j-1,j+1}$. Now suppose A_j is a p-basis of $L_{j-1,j+1}/L^p_{j,j+1}$. Then $A_j \cup T_{j-1,j}$ is a p-basis for $L_{j-1,j}/L^p_{j,j+1}$. Since $L^{p^2}_{j+1} \subseteq L^p_j$,

$$L_j^p(A_j) = L_j^p(L_{j-1}^p(L_{j+1}^{p^2})(A_j))$$

$$= L_j^p(L_{j,j+1}^p)(A_j)$$

$$= L_j^p(L_{j-1,j+1})$$

$$= L_{j-2}(L_j^p)$$

$$= L_{j-1,j}.$$

Thus we can and do choose a p-basis $A_j^* \subseteq A_j$ of

$$L_{j-1,j}/L_j^p.$$

Then $A_j^* \cup T_{j,j}^p$ is a p-basis of

$$L_{j-1,j}/L_{j,j+1}^p.$$

Similarly $A_j \cup T_{j-1,j}^!$ and $A_j^* \cup T_{j,j}^{!p}$ are p-bases of

$$L_{j-1,j}/L_{j,j+1}^p.$$

Thus $(T^p_{j,j} - T_{j-1,j})$ and $(A_j - A^*_j)$ are p-bases for

$$L_{j-1,j}/L^p_{j,j+1}(T_{j-1,j}, A^*_j),$$

while $(T'^p_{j,j} - T'_{j-1,j})$ and $(A_j - A^*_j)$ are p-bases for

$$L_{j-1,j}/L^p_{j,j+1}(T'_{j-1,j}, A^*_j).$$

Hence we must have

$$|T^p_{j,j} - T_{j-1,j}| = |A_j - A^*_j| = |T'^p_{j,j} - T'_{j-1,j}|.$$

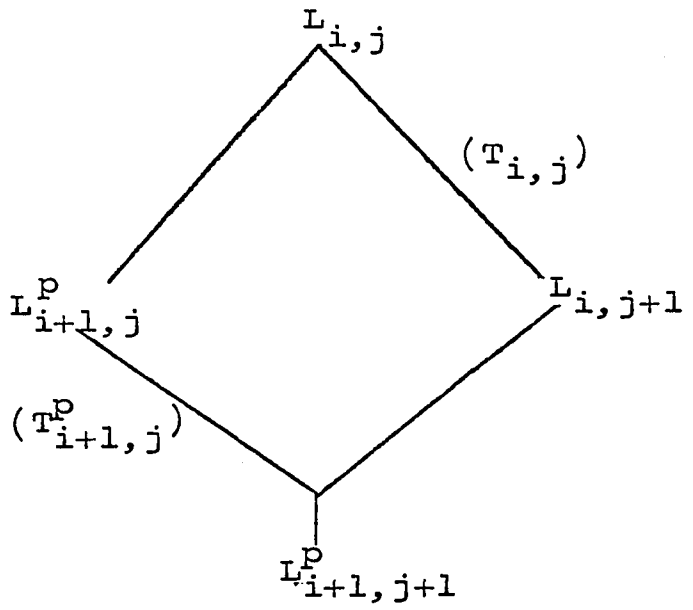
Now suppose that $i < j$. Then $T_{i,j}$ and $T'_{i,j}$ are p-bases for

$$L_{i,j}/L_{i,j+1}$$

and $T^p_{i+1,j}$ and $T'^p_{i+1,j}$ are p-bases for

$$L^p_{i+1,j}/L^p_{i+1,j+1}.$$

We have the lattice diagram:



Let A_i be a p-basis of

$$L_{i,j+1}/L^p_{i+1,j+1}.$$

Thus $A_i \cup T_{i,j}$ is a p-basis of

$$L_{i,j}/L^p_{i+1,j+1}.$$

Now

$$L_{j+1}^{p^{j+1-i}} \subseteq L_j^{p^{j-i}}$$

implies

$$L^p_{i+1,j-1}(T^p_{i+1,j}, A_i) = L^p_{i+1,j}(A_i)$$

$$= L^p_i(L^{p^{j+1-i}}_{j+1})(A_i)(L^{p^{j-i}}_j)$$

$$= L^p_{i+1,j+1}(A_i)(L^{p^{j-i}}_j)$$

$$= L_{i,j+1}(L^{p^{j-i}}_j)$$

$$= L_{i,j}.$$

Thus we can choose a p-basis $A^*_i \subseteq A_i$ of $L_{i,j}/L^p_{i+1,j}$. Then $T^p_{i+1,j} \cup A^*_i$ is a p-basis of

$$L_{i,j}/L^p_{i+1,j+1}.$$

Similarly $T'_{i,j} \cup A_i$ and $T'^p_{i+1,j} \cup A^*_i$ are p-bases of

$$L_{i,j}/L^p_{i+1,j+1}.$$

Hence $(T^p_{i+1,j} - T_{i,j})$ and $(A_i - A^*_i)$ are p-bases of

$$L_{i,j}/L^p_{i+1,j+1}(A^*_i, T_{i,j})$$

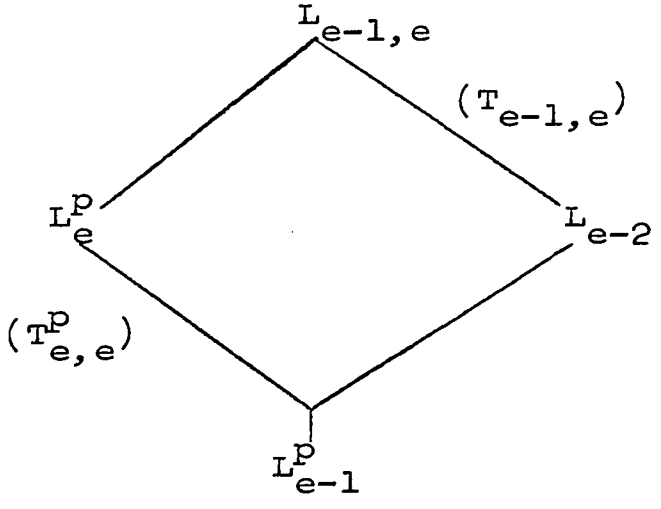
and $(T'^{p}_{i+1,j} - T'_{i,j})$ and $(A_i - A^*_i)$ are p-bases of

$$L_{i,j}/L^{p}_{i+1,j+1}(A^*_i, T'_{i,j}).$$

Thus

$$|T^{p}_{i+1,j} - T_{i,j}| = |A_i - A^*_i| = |T'^{p}_{i+1,j} - T'_{i,j}|.$$

Hence (2) is true for every (i,j), where $i \leq j$ and $j > 1$. If $j = 1$ (2) is trivial. If $L^{p^e} \subseteq K$ we have a special case when $j = e$. In this case $T^{p}_{e,e}$ is a p-basis of L^{p}_{e}/L^{p}_{e-1} and $T_{e-1,e}$ is a p-basis of $L_{e-1,e}/L_{e-2}$. Thus we have the lattice diagram:



An argument completely similar to the above gives the desired result. Q.E.D.

Definition 5.2. If $x \in T_{j,j}$, then the length of x, denoted by $\ell(x)$, is defined by

$$\ell(x) = \max\{k : x^{p^k} \in T_{j-k,j}\}.$$

The length of $T_{j,j}$, denoted by $\ell(T_{j,j})$, is defined by

$$\ell(T_{j,j}) = \max\{\ell(x) : x \in T_{j,j}\}.$$

We notice that $|T^p_{i+1,j} - T_{i,j}|$ is the number of elements in $T_{j,j}$ of length $j - i - 1$. Also it is clear from the definition that $T_{j-\ell_j,j}$, where $\ell_j = \ell(T_{j,j})$, is the last nonempty element of the j-th column of the tower triangle.

Corollary 5.3. If T and T' are tower sets of L/K. Then there exists a one-one onto function $g : T \to T'$ such that if $x \in T$, $\ell(x) = \ell(g(x))$.

Proof: For any integer $j \geq 1$ there exists a one-one onto function $g_{1,j} : T_{1,j} \to T'_{1,j}$. Suppose this map has been extended to a one-one onto map $g_{n,j} : T_{n,j} \to T'_{n,j}$. Now

$$|T^p_{n+1,j}| = |T_{n+1,j}| = |T'_{n+1,j}| = |T'^p_{n+1,j}|$$

and

$$|T^{p}_{n+1,j} - T_{n,j}| = |T'^{p}_{n+1,j} - T'_{n,j}|$$

by the theorem. Hence $g_{n,j}$ can be extended to a one-one onto map

$$g_{n+1,j} : T_{n+1,j} \to T'_{n+1,j}.$$

Thus there exists a one-one onto map $g_{j,j} : T_{j,j} \to T'_{j,j}$. For $j \neq k$, $T_{j,j} \cap T_{k,k} = \emptyset$, hence

$$g = \bigcup_{j=1}^{\infty} g_{j,j}$$

defines a one-one onto map $g : T \to T'$ such that $x \in T_{j,j}$ implies $g(x) \in T'_{j,j}$. Then by the construction of $g_{j,j}$ it is clear that $\ell(x) = \ell(g(x))$.

Definition 5.4. If τ is any tower triangle of L/K then the numbers $|T|$, $|T_{i,j}|$, $|T^{p}_{i+1,j} - T_{i,j}|$, and $\ell(T_{j,j})$, $j = 1,2,\ldots$, $i = j, j+1, \ldots$ will be called the tower invariants of L/K. If in addition τ is a tower generating triangle these numbers will be called tower generating invariants.

Proposition 5.5. If τ is a tower triangle such that for each i,

$$\bigcup_{j=i}^{\infty} T_{i,j}$$

is a p-basis of L_i/L_{i-1} and $x \in T_{j,j}$ implies $\ell(x) = j-1$ then

$$T = \bigcup_{j=1}^{\infty} T_{j,j}$$

is a subbasis for L/K.

Proof: The monomials of the form

$$\prod_{x \in T} x^{e(x)}, \quad 0 \leq e(x) < p^{\ell(x)+1} = p^j$$

where all but a finite number of $e(x)$ are zero, is a linear basis for L/K. Q.E.D.

Proposition 5.6. If L/K has a subbasis, and τ is a tower triangle such that for each i,

$$\bigcup_{j=i}^{\infty} T_{i,j}$$

is a p-basis of L_i/L_{i-1}, then T is a subbasis. In

particular if $L^{p^e} \subseteq K$ and L/K has a subbasis every tower set is a subbasis.

Proof: It is proved in [1] and [5] that L/K has a subbasis if and only if L^{p^i} and K are linearly disjoint over $L^{p^i} \cap K$, $i = 1,2,\ldots$. (This result is also proved in [9] when $L^{p^e} \subseteq K$.) If we show that for each $x \in T_{j,j}$, $\ell(x) = j$, then Proposition 5.5 gives the result. It suffices to show that if S is a p-independent subset of L_i/L_{i-1} then S^p is a p-independent subset of L_{i-1}/L_{i-2} To do this we show $\{ \pi_{t \in S} t^{pe(t)} : 0 \leq e(t) < p$ and $e(t) = 0$ for all but a finite number of $t\}$ is linearly independent over L_{i-2}. Suppose there exist

$$a_1,\ldots,a_n \in L_{i-2}$$

such that

$$\sum_{j=1}^{n} a_j \pi_j t^{pe(t)} = 0.$$

Then

$$\left(\sum_{j=1}^{n} a_j \pi_j t^{pe(t)} \right)^{p^{i-2}} = \sum_{j=1}^{n} a_j^{p^{i-2}} \pi_j t^{p^{i-1} e(t)} = 0$$

Now $a_j^{p^{i-2}} \in K$ so this is a dependence relation over K. Since K and L^{p^i} are linearly disjoint over $K \cap L^{p^i}$ there exists a dependence relation

$$\sum_{j=1}^{n} b_j \pi_j t^{p^{i-1}} e(t) = 0$$

with $b_j \in K \cap L^{p^i}$. Then

$$\sum_{j=1}^{n} b_j^{p^{1-i}} \pi_j t^{e(t)} = 0$$

with

$$b_j^{p^{1-i}} \in K^{p^{1-i}} \cap L = L_{i-1}.$$

This contradicts the p-independence of S over L_{i-1}.

Q.E.D.

VI. TOWER SETS AND LATTICE ISOMORPHISMS

If L/K and L'/K are two extensions of K, and τ and τ' are respective tower triangles, we say that L/K and L'/K have the same tower invariants if $|T_{i,j}| = |T'_{i,j}|$, $|T^p_{i+1,j} - T_{i,j}| = |T'^p_{i+1,j} - T'_{i,j}|$, and $\ell(T_{j,j}) = \ell(T'_{j,j})$, where $T_{i,j}$ and $T'_{i,j}$ denote the (i,j)-th entry of τ and τ' respectively.

Theorem 6.1. If L/K and L'/K are two extensions such that $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic, L/K and L'/K have the same tower invariants.

Proof: Let f denote the isomorphism of $\mathfrak{L}$ to $\mathfrak{L}'$ and let $j \geq 1$ be a given integer. (If $L^{p^e} \subseteq K$ then $j < e$.) By Theorem 2.11

$$f(L_j) = L'_j$$

and

$$f(L_{j,j+1}) = L'_{j,j+1}.$$

Since $T_{j,j}$ is a p-basis of $L_j/L_{j,j+1}$, Theorem 2.7 implies there exists a p-basis $T'_{j,j}$ of $L'_j/L'_{j,j+1}$ such that $t' \in T'_{j,j}$ implies there exists $t \in T_{j,j}$ such that

$$f(L_{j,j+1}(t)) = L'_{j,j+1}(t').$$

Now suppose for $1 \leq n < j - 1$ we have constructed a sequence of sets

$$T'_{j,j}, T'_{j-1,j}, \ldots, T'_{j-n,j}$$

with the following property:

(*) $T'_{j-k,j} \subseteq T'^{p}_{j-k+1,j}$ is a p-basis of $L'_{j-k,j}/L'_{j-k,j+1}$, $|T_{j-k,j}| = |T'_{j-k,j}|$, $|T^{p}_{j-k+1,j} - T_{j-k,j}| = |T'^{p}_{j-k+1,j} - T'_{j-k,j}|$, and $t' \in T'_{j-k,j}$ implies there exists $t \in T_{j-k,j}$ such that $f(L_{j-k,j+1}(t)) = L'_{j-k,j+1}(t')$.

We wish to construct a p-basis

$$T'_{j-n-1} \subseteq T'^{p}_{j-n,j}$$

with property (*), where $k = n + 1$. To this end let $t' \in T'_{j-n,j}$. By hypothesis there exists a $t \in T_{j-n,j}$ such that

$$f(L_{j-n,j+1}(t)) = L'_{j-n,j+1}(t'),$$

and by Theorem 2.11

$$f(L_{j-n-1,j+1}) = L'_{j-n-1,j+1}.$$

Then since $L^p_{j-n-1} \subseteq L_{j-n-2}$ we have by Lemma 2.10 that

$$f(L_{j-n-1,j+1}(t^p)) = L'_{j-n-1,j+1}(t'^p).$$

Thus for each $t \in T_{j-n-1,j}$ we can and do select a $t' \in T'_{j-n,j}$ such that

$$f(L_{j-n-1,j+1}(t)) = L'_{j-n-1,j+1}(t'^p).$$

Let $T'_{j-n-1,j}$ be the set of p-th powers of the set of t''s so selected. Using the by now familiar l.u.b. argument we have

$$f(L_{j-n-1,j}) = f(L_{j-n-1,j+1}(T_{j-n-1,j})$$

$$= L'_{j-n-2}(L^{p^{n+2}}_{j+1})(T'_{j-n-1,j})$$

$$= L'_{j-n-1,j+1}(T'_{j-n-1,j})$$

$$= L'_{j-n-1,j}.$$

Furthermore, since f is an isomorphism and $T_{j-n-1,j}$ is a m.g.s., we must have $T'_{j-n-1,j}$ is a m.g.s., and hence a p-basis. By construction it is clear that

$$|T'_{j-n-1,j}| = |T_{j-n-1,j}|$$

and

$$|T'^{p}_{j-n,j} - T'_{j-n-1,j}| = |T^{p}_{j-n,1} - T_{j-n-1,j}|.$$

Thus for each integer j we can construct the sequence of sets

$$T'_{j,j}, T'_{j-1,j}, \ldots, T'_{1,j}$$

with property (*).

Now if $L^{p^e} \not\subseteq K$, letting j range over the positive integers we get a tower triangle construction τ' for L'/K. If $L^{p^e} \subseteq K$ we have a special case when $j = e$. In this case $T_{e,e}$ is a p-basis of L_e/L_{e-1}, and the construction of

$$T'_{e,e}, T'_{e-1,e}, \ldots, T'_{1,e}$$

is totally similar to the construction given above.

Since for each j the sequence satisfies property (*), it is apparent that if $T_{k,j} = \emptyset$ then $T'_{k,j} = \emptyset$ for $1 \leq k \leq j$ and hence

$$\ell(T_{j,j}) = \ell(T'_{j,j}).$$

Q.E.D.

Suppose τ is a tower generating triangle for L/K, and $\mathfrak{L}$ and $\mathfrak{L}'$ are isomorphic. Given any $a' \in L'$ such that $\exp a'/K = k$, we must have an $a \in f^{-1}(K(a'))$ such that $\exp a/K = k$, and $f(K(a)) = K(a')$ by Lemma 2.6. Then

$$a \in K\left(\bigcup_{i=1}^{j} T_{i,i}\right)$$

for some $j > 0$. If we construct τ' as in Theorem 6.1, Lemma 2.11 and a typical l.u.b. argument show that

$$a' \in K(\bigcup_{i=1}^{j} T'_{i,i}).$$

Hence τ' is a tower generating triangle of L'/K.

We now show that the converse of Theorem 6.1 is not true.

Example 6.2. When L/K and L'/K have the same tower invariants, $\mathfrak{L}$ and $\mathfrak{L}'$ need not be isomorphic. Let P be a perfect field of characteristic $p \neq 0$, and w,x,y,z algebraically independent indeterminants over P. Let

$$K = P(w,x,y,z), \quad L = K(w^{p^{-1}}, z^{p^{-3}}, x^{p^{-1}} z^{p^{-3}} + y^{p^{-1}})$$

and

$$L' = K(y^{p^{-1}}, z^{p^{-3}}, x^{p^{-1}} z^{p^{-3}} + y^{p^{-2}}).$$

Then we have the refined right basic chains of $\mathfrak{L}$ and $\mathfrak{L}'$ as follows:

Refined Right Basic Chain of L/K

$$L = L_3 = P(x, y, w^{p^{-1}}, z^{p^{-3}}, x^{p^{-1}} z^{p^{-3}} + y^{p^{-1}})$$

$$L_2 = L_{2,3} = P(x, y, w^{p^{-1}}, z^{p^{-2}})$$

$$L_1 = P(x, y, w^{p^{-1}}, z^{p^{-1}})$$

$$L_{1,3} = L_{1,2} = P(w, x, y, z^{p^{-1}})$$

$$L_0 = K = P(w, x, y, z)$$

Refined Right Basic Chain of L'/K

$$L' = L'_3 = P(w, x, y^{p^{-1}}, z^{p^{-3}}, x^{p^{-1}} z^{p^{-3}} + y^{p^{-2}})$$

$$L'_2 = L'_{2,3} = P(w, x, y^{p^{-1}}, z^{p^{-2}})$$

$$L'_1 = P(w, x, y^{p^{-1}}, z^{p^{-1}})$$

$$L'_{1,2} = L'_{1,3} = P(w, x, y, z^{p^{-1}})$$

$$L'_0 = K = P(w, x, y, z)$$

Hence we have the tower triangles τ and τ' as follows:

τ

$$\{z^{p-3}, x^{p-1}z^{p-3} + y^{p-1}\}$$

$$\emptyset \qquad \{z^{p-2}\}$$

$$\{w^{p-1}\} \qquad \emptyset \qquad \{z^{p-1}\}$$

τ'

$$\{z^{p-3}, x^{p-1}z^{p-3} + y^{p-2}\}$$

$$\emptyset \qquad \{z^{p-2}\}$$

$$\{y^{p-1}\} \qquad \emptyset \qquad \{z^{p-1}\}$$

The set

$$\{z^{p-3}, x^{p-1}z^{p-3} + y^{p-1}, w^{p-1}\}$$

is a m.g.s. for L/K. However, since

$$y^{p^{-1}} = (x^{p^{-1}} z^{p^{-3}} + y^{p^{-2}})^p - xz^{p^{-2}},$$

the set

$$\{z^{p^{-3}}, x^{p^{-1}} z^{p^{-3}} + y^{p^{-2}}\}$$

is a m.g.s. for L'/K. Hence Theorem 2.7 shows that $\mathfrak{L}$ and $\mathfrak{L}'$ cannot be isomorphic.

VII. REFERENCES

1. Haddix, G., Mordeson, J. and Vinograde, B. On purely inseparable extensions of unbounded exponent. To be published ca. 1969.

2. Hamman, E. and Mordeson, J. Pure inseparable field extensions. Mathematische Zeitschrift 103: 43-47. 1968.

3. Jacobson, N. Lectures in abstract algebra. Vol. 3. Princeton, N. J., D. Van Nostrand Co., Inc. 1964.

4. Mordeson, J. and Vinograde, B. Tensor products of simple pure inseparable field extensions. American Mathematical Society Proceedings ca. 1969.

5. Mordeson, J. and Vinograde, B. Generators and tensor factors of purely inseparable fields. Mathematische Zeitschrift ca. 1969.

6. Pickert, G. Inseparable korperwieterungen. Mathematische Zeitschrift 52: 81-136. 1949.

7. Pickert, T. Zwischenkorperverbande endlicher inseparabler Erweiterungen. Mathematische Zeitschrift 55: 355-363. 1952.

8. Rygg, P. On minimal sets of generators of purely inseparable field extensions. American Mathematical Society Proceedings 14: 742-745. 1963.

9. Sweedler, M. Structure of inseparable extensions. Annals of Mathematics 87: 401-410. 1968.

10. Wiesfeld, M. Purely inseparable extensions and higher derivations. American Mathematical Society Transactions 116: 435-449. 1965.

11. Zariski, O. and Samuel, P. Commutative algebra. Vol. 1. Princeton, N. J., D. Van Nostrand Co., Inc. 1958.

VIII. ACKNOWLEDGMENT

The author wishes to express his gratitude to Dr. Bernard Vinograde and Dr. John Mordeson of The Creighton University for their generous assistance and instruction in the preparation of this thesis.